1. A method for countering invasive software activity, the method comprising:

detecting invasive executables in a software system;

installing a counter-invasive software application (CISA) to create evidence of invasive activity conducted as a result of the invasive executable;

taking remedial action against an obligor to obtain an obligation therefrom; and

monitoring compliance by the obligor with respect to the obligation.

2. The method of claim 1, wherein the software system is provided by a supplier and hosted by a service provider.

3. The method of claim 2, wherein the obligor is at least one of the supplier and the service provider.

4. The method of claim 2, further comprising contacting at least one of the supplier and the service provider to obtain cooperation in defeating the invasive executable.

5. The method of claim 4, further comprising motivating at least one of the supplier and service provider to provide a solution for defeating the invasive executable.

6. The method of claim 5, further comprising motivating at least one of the supplier and service provider to develop the solution.

7. The method of claim 1, further comprising motivating the obligor to provide a solution rendering ineffectual the invasive executable.

8. The method of claim 7, wherein motivating is the remedial action.

9. The method of claim 2, further comprising installing the CISA on a computer of the service provider.

10. The method of claim 2, further wherein installing further comprises installing the CISA on a computer remote from and not under the control or knowledge of the service provider in order to monitor the service provider for breaches of duty due from the service provider to a client thereof and breached as a result of the invasive executable.

11. The method of claim 2, further comprising providing test information to the service provider, the test information containing a characteristic identifiable to substantiate the invasive activity by the invasive executable.

12. The method of claim 11, further comprising providing the test information without informing the service provider concerning the characteristic thereof.

13. The method of claim 12, further comprising:

collecting evidence of the activity of the invasive software;

evaluating the evidence to determine the adequacy thereof to support a demand for remedial action against at least one of the service provider and the supplier.

14. The method of claim 13, further comprising:

continuing collecting additional evidence;

determining the adequacy of the evidence is sufficient; and

taking remedial action against at least one of the supplier and the service provider.

15. The method of claim 14, wherein at least one of the supplier and service provider is the obligor.

16. The method of claim 1, further comprising developing solution software to mitigate at least one effect of the invasive executable.

17. The method of claim 1, further comprising obtaining a right to monitor activity of the invasive executable on a computer corresponding to a service supplier hosting the software system.

18. The method of claim 1, wherein installing further comprises installing the CISA on a computer corresponding to a party other than the obligor.

19. The method of claim 18, further comprising :

executing the CISA to create tracking data corresponding to the invasive activity of the invasive executable; and

collecting the tracking data to create evidence of the invasive activity.

20. The method of claim 19, further comprising providing, in response to the activity of the invasive software, witness data originating from the CISA to be stored to evidence the origination thereof from the CISA.

21. The method of claim 20, further comprising:

creating by the CISA witness data to be stored to evidence the origination thereof from the CISA; and

providing to a target party, in response to the activity of the invasive software, the witness data.

22. The method of claim 21, wherein the target party is the obligor.

23. The method of claim 21, wherein:

taking remedial action further comprises filing an action against the obligor.

24. The method of claim 23, further comprising obtaining in discovery at least a portion of the witness data.

25. The method of claim 1, further comprising obtaining a status as at least one of a class member, a shareholder, a customer, and a client with respect to a source of the invasive executable.

26. The method of claim 2, further comprising obtaining a status as at least one of a class member, a shareholder, a customer, and a client with respect to at least one of the supplier and the service provider.

27. The method of claim 1, wherein taking remedial action further comprises filing at least one of a class action, a shareholder action, and an individual action.

28. A method for countering invasive software, the method comprising:

procuring an invasive software system (ISS) provided by a supplier and configured to invasively obtain and communicate to the supplier proprietary information from a computer of a user, the proprietary information giving rise to a duty of non-disclosure thereof;

testing the product to determine invasive operation thereof;

developing, a counter-invasive software application (CISA) to do at least one of detecting, ameliorating, and defeating the operation of the invasive software system.

29. The method of claim 28, further comprising motivating a source of the ISS to do at least one of developing a solution effective to provide protection against the invasive activity of the ISS while leaving substantially operational legitimate operations of the ISS and modifying the ISS to render it ineffective.

30. The method of claim 28, wherein the ISS comprises a computer operating system.

31. The method of claim 28, wherein the CISA is programmed to create evidence of invasive activity.

32. The method of claim 28, wherein the CISA is programmed to create tracking data to monitor attempts by the ISS to conduct invasive activity.